

【特許請求の範囲】

【請求項1】個人証の識別子と、この識別子にかかる電子透かし情報とを対応付けて記憶するデータベースと、前記データベースに記憶された識別子を持ち、かつ、この識別子にかかる電子透かしが埋め込まれた認証画像を読み取り可能に担持する個人証と、前記個人証から少なくとも認証画像を読み出す読出手段と、

前記データベースから前記個人証の識別子に対応する電子透かし情報を取り出す透かし情報問合せ手段と、前記読出手段が読み出した認証画像に、前記透かし情報問合せ手段が取り出した電子透かし情報が埋め込まれているかどうか検討し、埋め込まれているとき前記個人証は正当と判定し、そうでないとき不正と判定する透かし情報比較手段とを備えたことを特徴とする正当性認証システム。

【請求項2】前記個人証には、認証画像を記憶する情報担体が設けられ、この情報担体が記憶する認証画像に、電子透かしが埋め込まれていることを特徴とする請求項1記載の正当性認証システム。

【請求項3】前記情報担体は、半導体メモリ又は磁性体の一方又は双方であることを特徴とする請求項2記載の正当性認証システム。

【請求項4】前記個人証には、認証画像を印刷した印刷物が貼り付けられ、前記読出手段は、この印刷物の画像入力を行うことを特徴とする請求項2記載の正当性認証システム。

【請求項5】前記電子透かし情報には、ランダムな値が含まれていることを特徴とする請求項1から4記載の正当性認証システム。

【請求項6】前記データベースが記憶し、かつ、前記個人証の認証画像に埋め込まれる電子透かし情報は、前記透かし情報比較手段が正当であると判定する都度、更新されることを特徴とする請求項1から5記載の正当性認証システム。

【請求項7】前記透かし情報問合せ手段は、通信網を介して前記データベースと通信することを特徴とする請求項1から6記載の正当性認証システム。

【請求項8】個人証に対してユニークな識別子を生成する識別子生成手段と、前記識別子生成手段が生成した識別子に対応する電子透かし情報を生成する透かし情報生成手段と、個人証の識別子と、この識別子にかかる電子透かし情報とを、対応付けて記憶するデータベースと、前記識別子生成手段が生成した識別子と、前記透かし情報生成手段が生成した電子透かし情報とを、前記データベースに記憶させる透かし情報登録手段と、生の認証画像を入力する顔画像入力手段と、前記顔画像入力手段が入力した認証画像に、電子透かしを埋め込んだ透かし入り認証画像を作成する透かし入り

画像作成手段と、

前記透かし入り画像作成手段が作成した透かし入り認証画像と、前記識別子生成手段が生成した識別子とを、読み取り可能に担持する個人証とを備えたことを特徴とする個人証発行システム。

【請求項9】前記個人証には、認証画像を記憶する情報担体が設けられ、この情報担体が記憶する認証画像に、電子透かしが埋め込まれていることを特徴とする請求項7記載の個人証発行システム。

【請求項10】前記情報担体は、半導体メモリ又は磁性体の一方又は双方であることを特徴とする請求項9記載の個人証発行システム。

【請求項11】前記個人証には、認証画像を印刷した印刷物が貼り付けられていることを特徴とする請求項9記載の個人証発行システム。

【請求項12】前記電子透かし情報には、ランダムな値が含まれていることを特徴とする請求項8から11記載の個人証発行システム。

【請求項13】前記データベースが記憶し、かつ、前記個人証の認証画像に埋め込まれる電子透かし情報は、所定時に更新されることを特徴とする請求項15記載の個人証発行システム。

【請求項14】前記透かし情報登録手段は、通信網を介して前記データベースと通信することを特徴とする請求項8から13記載の個人証発行システム。

【請求項15】固有の識別子を持ち、かつ持ち主の認証画像が目視可能に表示される個人証であって、前記認証画像には、前記識別子に対応する電子透かし情報が埋め込まれ、しかも、この識別子と、この電子透かし情報とは、この個人証から離れたデータベースに対応付けて記憶されていることを特徴とする個人証。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、正当性認証システム、個人証発行システム及びこれらのシステムで用いられる用いられる個人証に関するものである。

【0002】

【従来の技術】一般に、クレジットカード、キャッシュカード、会員証、学生証、社員証、パスポート、保険証、免許証などのように、認証画像を含む個人証（形態は、カード型またはブック型などがある）が、広く用いられている。ここで、本明細書において、「認証画像」とは、例えば、顔写真画像、指紋又は瞳の画像など、個人を特定できる画像をいう。

【0003】ところが、これらの個人証の持ち主でないものが、認証画像を持ち主の認証画像から違う認証画像にすり替えて、あたかも持ち主であるかのように、なりすまし事件が多発しており、社会的な問題になっている。

【0004】これについての対策として、顔写真に電子

透かしを埋め込む技術が提案されている(特開平10-275203号公報)。電子透かしを用いると、デジタルデータである認証画像に、所望のデータを、目では見えないように、透かし情報を埋め込むことができる。

【0005】そして、このものでは、個人証に電子透かしを埋め込み、認証機器(カードリーダーなど)側で正しく電子透かしを取り出せるかどうかにより、個人証の正当性を判断している。

【0006】また、一般に、個人証作成時に、持ち主の識別子が「BBB」であり、追加する情報が「AAA」であるとき、「ABABAB」という電子透かしが埋め込む場合を考える。

【0007】この場合、認証時には、認証画像から、電子透かしを読み込む。読み込みに失敗すれば、不正と判断される。また、読み込みに成功しても、埋め込み時と逆の手順で、「ABABAB」から識別子「BBB」を除いた、情報「AAA」を分離し、これが正しいかどうか検討される。検討の結果、正しいとされれば、正当と判断され、そうでなければ、不正と判断される。

【0008】

【発明が解決しようとする課題】しかしながら、従来技術では、カード上のデータのみで、正当性を判断しており、電子透かしを埋め込むアルゴリズムが、漏れるか、又は、見破られてしまうと、簡単に改竄されてしまうという問題点があった。例えば、Aさんのクレジットカードを盗んだ、犯人Bが、B自身の顔写真に、このアルゴリズムに従う、電子透かしを埋め込んだ顔写真を貼り、犯人Bが、このクレジットカードを利用して、買い物をして、犯人Bの不正を暴くことができない。このように、従来技術では、セキュリティの上の問題が避けられなかった。

【0009】そこで本発明は、安全性が高い正当性認証システム、個人証発行システム及びこれらのシステムで用いられる用いられる個人証を提供することを目的とする。

【課題を解決するための手段】本発明の正当性認証システムは、個人証の識別子と、この識別子にかかる電子透かし情報とを対応付けて記憶するデータベースと、データベースに記憶された識別子を持ち、かつ、この識別子にかかる電子透かしが埋め込まれた認証画像を読み取り可能に担持する個人証と、個人証から少なくとも認証画像を読み出す読出手段と、データベースから個人証の識別子に対応する電子透かし情報を取り出す透かし情報問合せ手段と、読出手段が読み出した認証画像に、透かし情報問合せ手段が取り出した電子透かし情報が埋め込まれているかどうか検討し、埋め込まれているとき個人証は正当と判定し、そうでないとき不正と判定する透かし情報比較手段とを備えている。

【0010】この構成により、安全性が高く堅牢なシステムを構築できる。

【0011】

【発明の実施の形態】請求項1、8、15の構成によると、認証画像に埋め込まれる電子透かし情報は、個人証の認証画像にあるというだけでなく、データベースによっても、記憶されているため、データベースに記憶されている電子透かし情報と、個人証から取り出された電子透かし情報とを、比較対応することにより、正当な使用のみを許すことができる。

【0012】例えば、犯人Bが盗んだ個人証の顔写真にうまく電子透かし情報を埋め込めても、データベース自体は改変されないから、データベースとの比較が不首尾に終わることとなり、犯人Bの不正を暴くことができる。即ち、個人証の認証画像のみに依存する場合に比べ、大幅に安全性を向上することができる。

【0013】請求項2、9の構成によると、電子透かしが情報担体に記憶されており、デジタルデータのまま読み出すことができるため、正確に電子透かし情報の比較を行える。

【0014】請求項3、10の構成によると、情報担体が、半導体メモリ又は磁性体であるため、個人証の重量を大幅に増加せずとも、記憶ができる。

【0015】請求項4、11の構成によると、印刷物に認証画像が印刷されているため、個人証を、薄くかつ軽くすることができる。

【0016】請求項5、12の構成によると、電子透かし情報には、ランダムな値が含まれているため、偽造、変造を試みる輩にとって、予測不能とすることができ、改竄をより困難にすることができる。

【0017】請求項6、13の構成によると、データベースと個人証の、顔写真情報に埋め込まれる電子透かし情報が、正当であると判定される都度、更新されることにより、改竄に対してより強い体制がとれる。

【0018】請求項7、14の構成によると、通信網を介して、データベースは、個人証が利用される位置から離れた位置にあり、データベースにアクセスできない限り、電子透かし情報が外部に漏れることはないため、システムの安全性を向上できる。

【0019】次に図面を参照しながら、本発明の実施の形態を説明する。まず、各形態の説明に先立ち、図5を用いて、本発明による、識別子、電子透かし情報及びデータベースの関係を概説する。また以下、認証画像として、顔写真画像を用いる場合を、中心にして説明する。

【0020】図5に示すように、個人証5には、識別子1、認証画像4が設けられる。識別子1と電子透かし情報2は、一対一に対応しており、データベース3に記憶されている。この例では、識別子1は「123」、電子透かし情報2は「hoge hoge」である。

【0021】(実施の形態1)次に、図1を用いて、実施の形態1を説明する。図1は、本発明の実施の形態1におけるシステムのブロック図である。ここで、図1の

左上部に示す個人証10は、発行済みのものであり、認証に用いられる。また、図1の右上部に表示される個人証20は、発行用のものである。

【0022】個人証10は、顔写真などを表示する表示部12と、情報担体としてのメモリ13と、識別子11（ここでは「123」）とを、具備している。

【0023】また、メモリ13にアクセスするために、入出力ポート14が設けてある。ここで、画像を記憶する上で容量が十分であるならば、メモリ13の代わりに、情報担体として、磁性ストラップなどの磁性体を用いてもよい。

【0024】メモリ13には、電子透かし情報が埋め込まれた認証画像が記憶されており、必要に応じて、表示部12に表示できるようになっている。この表示部12は、例えば、LCDなどからなる。

【0025】また、発行用の個人証20にも、同様に、識別子21（ここでは「234」）、メモリ23、入出力ポート24が設けられている。以上が個人証の構成である。

【0026】次に、本形態のシステムについて説明する。なおこのシステムは、説明の便宜上、正当性認証システム、個人証発行システムとを、組み合わせたものとなっているが、正当性認証システム、個人証発行システムは、別々に構成することもできる。

【0027】さて、読出手段30は、入出力ポート14に接続されており、メモリ13に記憶され、電子透かし情報が埋め込まれた、認証画像を読み出す。

【0028】逆に、書込手段31は、入出力ポート24に接続されており、メモリ23に電子透かし情報が埋め込まれた顔写真情報を書き込む。

【0029】入力手段32は、個人証の認証あるいは発行の際に必要な情報入力を受け付ける。デジタルカメラ33は、持ち主の顔を撮影し、認証画像（デジタル）を出力する。制御手段34は、他の各要素を制御するとともに、個人証の正当性を判断する。

【0030】透かし情報抽出手段35は、読み出し手段30が読み出した認証画像から電子透かし情報のみを抽出し、制御手段34に返す。

【0031】透かし情報比較手段36は、データベース3から得た透かし情報と、透かし情報抽出手段35が抽出した透かし情報とを比較し、これらの透かし情報が一致するか否かを、制御手段34に返す。

【0032】透かし入り画像作成手段37は、後述するように、サーバ42側から得た、生成された透かし情報を、デジタルカメラ33が撮影した認証画像に埋め込んで、電子透かしが埋め込まれた認証画像を作成する。

【0033】透かし情報登録手段38は、データベース3に、識別子と、これに対応する電子透かしを登録するよう求める。透かし情報問合せ手段39は、データベース3に、識別子を渡し、これに対する透かし情報を問い合わせる。

通信手段40は、通信網41を経由して、サーバ42と通信を行う。

【0034】サーバ42には、識別子生成手段43と、透かし情報生成手段44とが設けられ、識別子生成手段43は、データベース3をアクセスして、要求に応じ、未だ付与されていないユニークな識別子を生成する。透かし情報生成手段44は、識別子に対応する透かし情報を作成する。

【0035】なお、この透かし生成の方式は、任意に決定して差し支えないが、規則性のないランダムな値（例えば、乱数値）を透かし情報に含めることが望ましい。このようにすると、改竄を試みる者（犯罪者またはそのグループ）にとって、予測がきわめて困難になり、システムの安全性をより向上できる。また、典型的には、透かし情報は、データベース3にテキストデータとして記録され、認証画像には、電子透かしとして埋め込まれる。

【0036】図1の例では、認証画像をデジタルカメラ33で撮影して取得しているが、印刷物をイメージスキャナなどで読みとって認証画像を入力してもよい。勿論、認証画像として、顔写真画像ではなく、指紋又は瞳の画像を採用するときは、それに合わせた入力手段を用いる。

【0037】また、識別子生成手段43、透かし情報生成手段44は、サーバ42側でなく、制御手段34側（サーバ42から見るとクライアント側）に設けてもよい。

【0038】（実施の形態2）次に、図2を参照しながら、実施の形態2におけるシステムについて説明する。このシステムは、個人証に、情報担体としてのメモリを設けない例であり、図1に示したものに対し、次の点が異なる。

【0039】認証用の個人証50には、識別子51（ここでは「123」）が表示されているが、情報担体はなく、当然、入出力ポートもない。その代わりに、印刷された顔写真52が、貼り付けてある。そして、これをイメージスキャナ70で入力するようになっている。

【0040】また、発行用の個人証60には、同様に、識別子61（ここでは「234」）が表示されるが、メモリ、入出力ポートはなく、顔写真62の貼付欄が形成されている。そして、プリンタ71によって、電子透かし情報が埋め込まれた、顔写真62が印刷され、これが上記貼付欄に貼り付けられる。その他の点は、図1の構成と同様である。

【0041】（処理）次に、図3を参照しながら、個人証を発行する処理の流れを説明する。なお、実施の形態2については、処理自体において、認証画像の読み出し・書き込みの要領が違っただけであり、以下、実施の形態1を中心に説明を行う。

【0042】まず、このシステムのオペレータ又は個人

証の持ち主が、必要な個人情報を、入力手段32を用いてシステムへ入力する(ステップ1)。次に、ステップ2にて、デジタルカメラ33により、持ち主を撮影し認証画像を取得する。

【0043】ステップ3では、制御手段34が、通信手段40を用いて、通信網41を経由し、サーバ42へ接続する。

【0044】次に、ステップ4にて、制御手段34は、通信手段40を経由し、サーバ42へ、識別子と、この識別子に対応する透かし情報を生成するように、要求する。

【0045】これに応じて、サーバ42側の、識別子生成手段43は、データベース3をアクセスし、未だ付与されていない新しい識別子を生成し、透かし情報生成手段44は、この新しい識別子に対応する透かし情報を生成し、これら識別子及び透かし情報が、制御手段34へ送信される(ステップ5)。

【0046】制御手段34は、以上の受信を行うと、透かし情報登録手段38を用いて、受信した識別子及び透かし情報を、データベース3に登録するように、要求させる(ステップ6)。この要求に応じて、サーバ42は、これらをデータベース3に記憶させてから、登録済み通知を制御手段34へ送信する(ステップ7)。

【0047】制御手段34は、この通知を受信すると、サーバ42との接続を解除し(ステップ8)、透かし入り画像作成手段37へ、受信した透かし情報と、デジタルカメラ33から得た認証画像とを、渡し、透かし入り画像が作成される(ステップ9)。

【0048】そして、ステップ10にて、以上のように作成された、透かし入り画像を書込手段31へ渡し、書込手段31は、入出力ポート24を介し、メモリ23にこの画像が書き込まれ、必要に応じて、認証画像が、表示部22に表示できるようになる。これにより、発行処理が完了する。

【0049】次に、図4を参照しながら、認証処理について説明する。いま、発行済みの個人証10が読出手段30にセットされたものとする。まず、読出手段30は、個人証10から識別子11(ここでは「123」)を読み出す(ステップ20)。なお、識別子などの入力は、入力手段32から行うようにしてもよい。

【0050】次に、ステップ21にて、読出手段30は、入出力ポート14からメモリ13に記憶されており、電子透かし情報が埋め込まれているはずの、認証画像を読み出す。

【0051】次に、ステップ22にて、制御手段34は、取得した認証画像を、透かし情報抽出手段35へ渡し、認証画像から透かし情報の抽出を行わせる。この抽出自体が失敗したときには(ステップ23)、制御手段34は、この個人証10は、不正であると判定し(ステップ24)、処理を終了する。

【0052】一方、透かし情報の抽出に成功したときには、制御手段34は、通信手段40を用いて、サーバ42に接続する(ステップ25)。

【0053】そして、制御手段34は、識別子11を、透かし情報問合せ手段39へ渡し、この識別子11に対応する、透かし情報の問い合わせを行わせる(ステップ26)。

【0054】サーバ42は、この問い合わせを受信すると、データベース3において、この識別子に対応する透かし情報を検索する。サーバ42は、もし見つからないなら、見つからない旨、見つかったら、見つかった透かし情報を、制御手段34へ返す(ステップ27)。

【0055】制御手段34は、サーバ42から受信すると、接続を解除する(ステップ28)。そして、制御手段34は、透かし情報が見つからなかった旨受信したときは(ステップ29)、この個人証10は、不正であると判定し(ステップ24)、処理を終了する。

【0056】一方、制御手段34は、透かし情報を受信したときは、透かし情報抽出手段35が抽出した透かし情報と、このときサーバ42から受信した透かし情報とを、透かし情報比較手段36へ渡し、比較を行わせる。透かし情報比較手段36による比較の結果、不一致となったときは、制御手段34は、この個人証10は、不正と判定して(ステップ24)、処理を終了する。

【0057】一方、この比較の結果、一致を見たときは、制御手段34は、この個人証10は、正当であると判定し(ステップ31)、処理を終了する。

【0058】また、正当であると判定できたときは、ステップ32にて、図3の要部と同様の処理をもう一度行い、この識別子に対応する透かし情報を、更新することが望ましい(ステップ32)。勿論、この更新は、個人証10の認証画像に埋め込まれる電子透かしの更新と、データベース3における電子透かしの更新との、両方(なお、これらの電子透かしは一致するようにする)を意味する。このようにすると、認証が成功する都度、電子透かしが更新され、一層、改竄に対して堅牢なシステムとすることができる。

【0059】

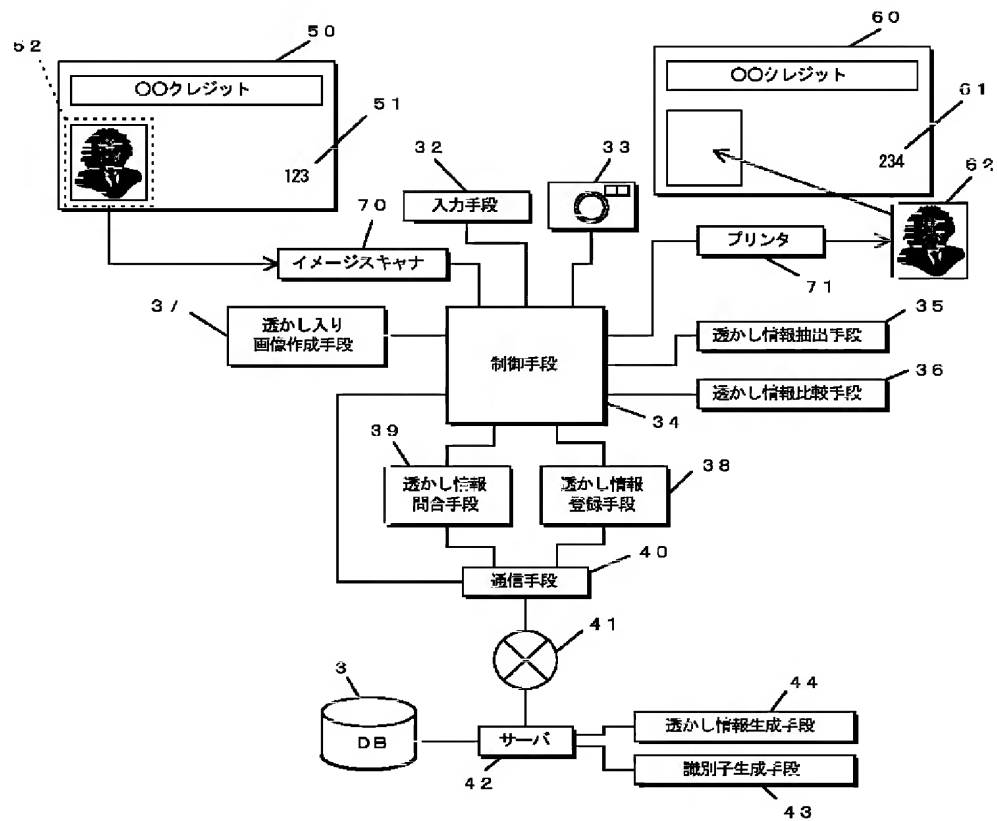
【発明の効果】本発明では、個人証の認証画像に埋め込まれた電子透かしを、認証機器で検証することのみに依存するのではなく、この電子透かしを、個人証や認証機器とは、別のデータベースでも記憶しておき、このデータベースの電子透かしとの突き合わせを併用しているため、認証画像の改竄、その他の不正使用に対して、堅牢なシステムを構築できる。

【図面の簡単な説明】

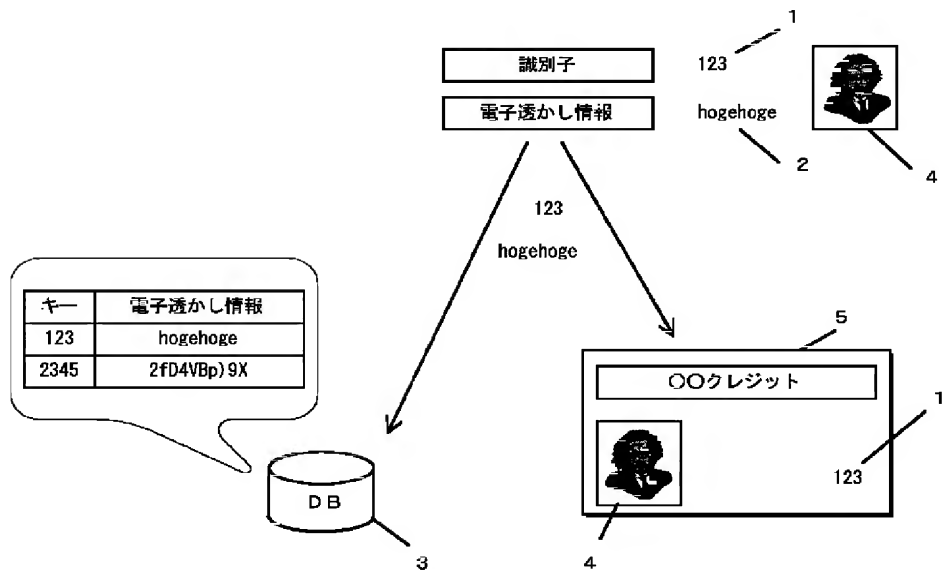
【図1】本発明の実施の形態1におけるシステムのブロック図

【図2】本発明の実施の形態2におけるシステムのブロック図

【図2】



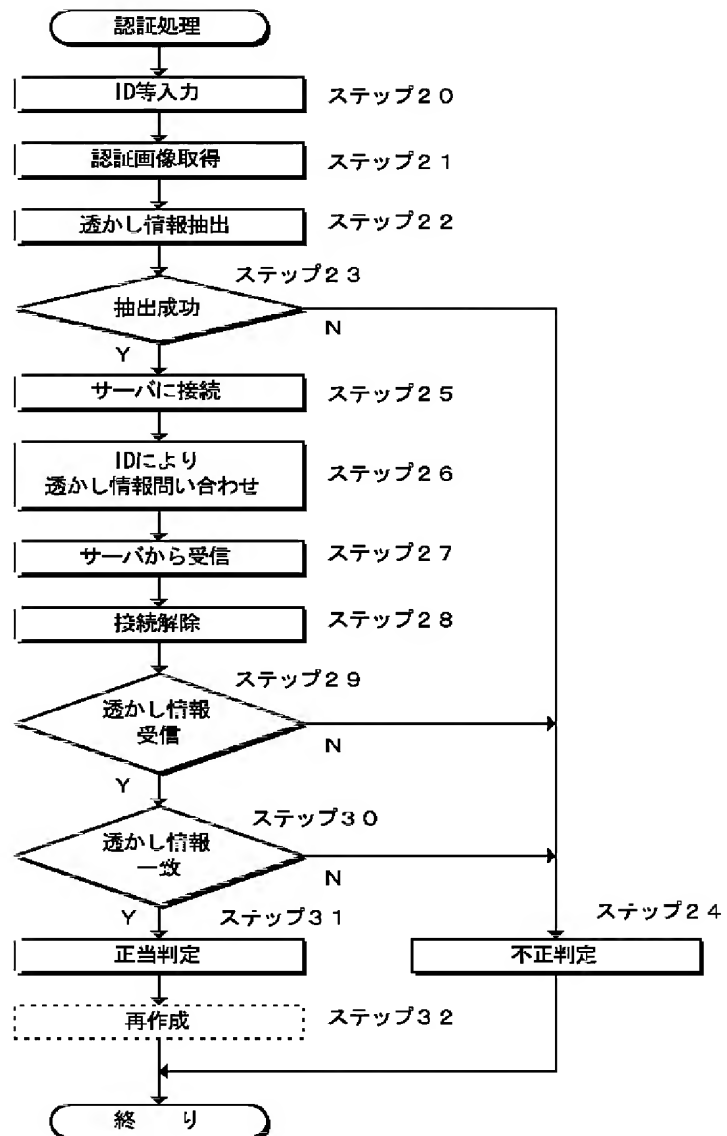
【図5】



【図3】



【図4】



フロントページの続き

(51)Int.Cl.⁷

識別記号

F I

H 0 4 L 9/00

6 7 3 C

(参考)

(72)発明者 津森 伸一

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 井上 尚

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 桂 卓史

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

F ターム(参考) 5B035 AA14 BB02 BB09 BB11 BC01
CA00
5B058 CA01 CA27 CA31 KA02 KA13
KA31 YA20
5C076 AA02 AA14 BA03 BA04
5J104 AA07 AA14 KA01 NA05 NA34
NA35 NA38 NA41